SPYWOLF

Security Audit Report

Completed on
July 13, 2023

OVERVIEW

This audit has been prepared for **Summer Doge** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

"

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

– SPYWOLF Team –

"

TABLE OF CONTENTS

Summer Doge

PROJECT DESCRIPTION

According to their whitepaper:

Welcome to SummerDoge! Immerse yourself in our exclusive community that combines the thrill of cryptocurrency trading with the joy of summer relaxation.

Discover TrendingSwap - our pioneering feature that empowers you with real-time, actionable insights into potential high-gain tokens. This summer is set to be unforgettable!

Release Date: Presale starts in July, 2023
Category: Meme token

CONTRACT INFO

Token Name
Summer Doge

Symbol
SUMDOGE

Contract Address
0xCe32660216913FC75ef6B9C5341eA80C0655a6c5

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Jul 10, 2023

Verified?
Yes

Total Supply
4,000,000

Status
Not launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	4000000 SUMDOGE
Median Transfer Amount	4000000 SUMDOGE
Average Transfer Amount	4000000 SUMDOGE
First transfer date	2023-07-10
Last transfer date	2023-07-10
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-07-10 09:06:49 UTC
Created	2023-07-10 09:06:49 UTC
Create TX	0x36cd8a7c7bb0d6ce445016ef6856a29aa8de6c8051efa67482a3babfbd55b660
Creator	0x36689bbfa3edc5746640ff91bdad52884b2bd581

03

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

04

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠️ High Risk

Owner can change sell limits.
When LimitSell is set to 0, users won't be able to sell their tokens.
When LimitSell is set to 1, users will be able to sell up to 100% of their tokens.
When LimitSell is set to 2, users will be able to sell up to 50% of their tokens per transaction.

```
function SetSell(uint LimitSell2) public onlyTeam{
    require(LimitSell2<=2,"Dump measure can't be under 50% of the wallet");
    LimitSell=LimitSell2;

    emit OnSetSell(LimitSell2);
}

function _taxedTransfer(address sender, address recipient, uint amount) private{
    uint senderBalance = _balances[sender];
    uint recipientBalance = _balances[recipient];
    require(senderBalance >= amount, "Transfer exceeds balance");
    require(senderBalance/LimitSell >= amount, "Transfer exceeds authorise sell");
    ...............................
}
```

- Recommendation:
  - Considered as good practice is max transaction limits (buy/sell/transfer) to be always greater or equal than 0.1% of total supply.

06-A

FOUND THREATS

⚠️ Low Risk

Owner can change contract's autoswap settings.
If swapTreshold is set to 0 and contract's token balances are 0,
transaction will be successful but contract won't be able to sell
tokens for BNB.

```
uint public swapTreshold=2;
    function setSwapTreshold(uint newSwapTresholdPermille) public onlyTeam{
    require(newSwapTresholdPermille<=15);//MaxTreshold= 1.5%
    swapTreshold=newSwapTresholdPermille;
}

function _swapContractToken(bool ignoreLimits) private lockTheSwap{
    uint contractBalance=_balances[address(this)];
    uint totalTax=liquidityTax+marketingTax;
    //swaps each time it reaches swapTreshold of pancake pair to avoid large prize impact
    uint tokenToSwap=_balances[_pancakePairAddress]*swapTreshold/1000;

    //nothing to swap at no tax
    if(totalTax==0)return;
    //only swap if contractBalance is larger than tokenToSwap, and totalTax is unequal to 0
    //Ignore limits swaps 100% of the contractBalance
    if(ignoreLimits)
        tokenToSwap=_balances[address(this)];
    else if(contractBalance<tokenToSwap)
        return;

    //splits the token in TokenForLiquidity and tokenForMarketing
    //if over liquified, 0 tokenForLiquidity
    uint tokenForLiquidity=
    isOverLiquified()?0
    :(tokenToSwap*liquidityTax)/totalTax;

    uint tokenForMarketing= tokenToSwap-tokenForLiquidity;

    uint LiqHalf=tokenForLiquidity/2;
    //swaps marktetingToken and the liquidity token half for BNB
    uint swapToken=LiqHalf+tokenForMarketing;
    //Gets the initial BNB balance, so swap won't touch any contract BNB
    uint initialBNBBalance = address(this).balance;
    _swapTokenForBNB(swapToken);
......................
}

function _swapTokenForBNB(uint amount) private {
    _approve(address(this), address(_pancakeRouter), amount);
    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = _pancakeRouter.WETH();

    try _pancakeRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(
        amount,
        0,
        path,
        address(this),
        block.timestamp
    ){}
    catch{}
}
```

- Recommendation:
  - Ensure that swapThreshold's value is always above 0.

06-B

ℹ️ Informational

There is initial bot protection for the first 30 seconds after owner trigger the SetupEnableTrading() function.
Taxes will start from 95% and will decrease gradually to the normal default taxes over the course of 30 seconds.

```solidity
uint public LaunchTimestamp;
function SetupEnableTrading() public onlyTeam{
    require(LaunchTimestamp==0,"AlreadyLaunched");
    LaunchTimestamp=block.timestamp;
    emit OnEnableTrading();
}

function _LimitlessFonctionTransfer (address sender, address recipient, uint amount) private{
......................
uint tax;
if(isSell){
    uint SellTaxDuration=30 seconds;
    if(block.timestamp<LaunchTimestamp+SellTaxDuration){
        tax=_getStartTax(SellTaxDuration,999);
        }else tax=sellTax;
    }
else if(isBuy){
    uint BuyTaxDuration=30 seconds;
    if(block.timestamp<LaunchTimestamp+BuyTaxDuration){
        tax=_getStartTax(BuyTaxDuration,999);
    }else tax=buyTax;
} else tax=transferTax;
......................
}

function _taxedTransfer(address sender, address recipient, uint amount) private{
......................
uint tax;
if(isSell){
    uint SellTaxDuration=30 seconds;
    if(block.timestamp<LaunchTimestamp+SellTaxDuration){
        tax=_getStartTax(SellTaxDuration,999);
        }else tax=sellTax;
    }
else if(isBuy){
    uint BuyTaxDuration=30 seconds;
    if(block.timestamp<LaunchTimestamp+BuyTaxDuration){
        tax=_getStartTax(BuyTaxDuration,999);
    }else tax=buyTax;
} else tax=transferTax;
......................
}

function _getStartTax(uint duration, uint maxTax) private view returns (uint){
    uint timeSinceLaunch=block.timestamp-LaunchTimestamp;
    return maxTax-((maxTax-50)*timeSinceLaunch/duration);
}
```

06-C

ⓘ Informational

Owner can set buy/sell/transfer fees up to 5%.
Combined buy+sell = 10%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function SetTaxes(uint buy, uint sell, uint transfer_, uint burn, uint marketing,uint liquidity) public onlyTeam{
    uint maxTax=(TAX_DENOMINATOR/MAXTAXDENOMINATOR)/2;
    require(buy<=maxTax&&sell<=maxTax&&transfer_<=maxTax,"Tax exceeds maxTax 5%");
    require(burn+marketing+liquidity==TAX_DENOMINATOR,"Taxes don't add up to denominator");

    buyTax=buy;
    sellTax=sell;
    transferTax=transfer_;
    marketingTax=marketing;
    liquidityTax=liquidity;
    burnTax=burn;
    emit OnSetTaxes(buy, sell, transfer_, burn, marketing,liquidity);
}
```

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function ExcludeAccountFromFees(address account, bool exclude) public onlyTeam{
    require(account!=address(this),"can't Include the contract");
    excludedFromFees[account]=exclude;
    emit ExcludeAccount(account,exclude);
}
```

Owner can exclude address from max sell/wallet limits.

```
function ExcludedFromLimit(address account, bool exclude) public onlyTeam{
    require(account!=address(this),"can't Include the contract");
    excludedFromLimit[account]=exclude;
    emit ExcludeAccountLimit(account,exclude);
}
```

06-D

RECOMMENDATIONS FOR
GOOD PRACTICES

1. Consider fundamental tradeoffs

2. Be attentive to blockchain properties

3. Ensure careful rollouts

4. Keep contracts simple

5. Stay up to date and track development
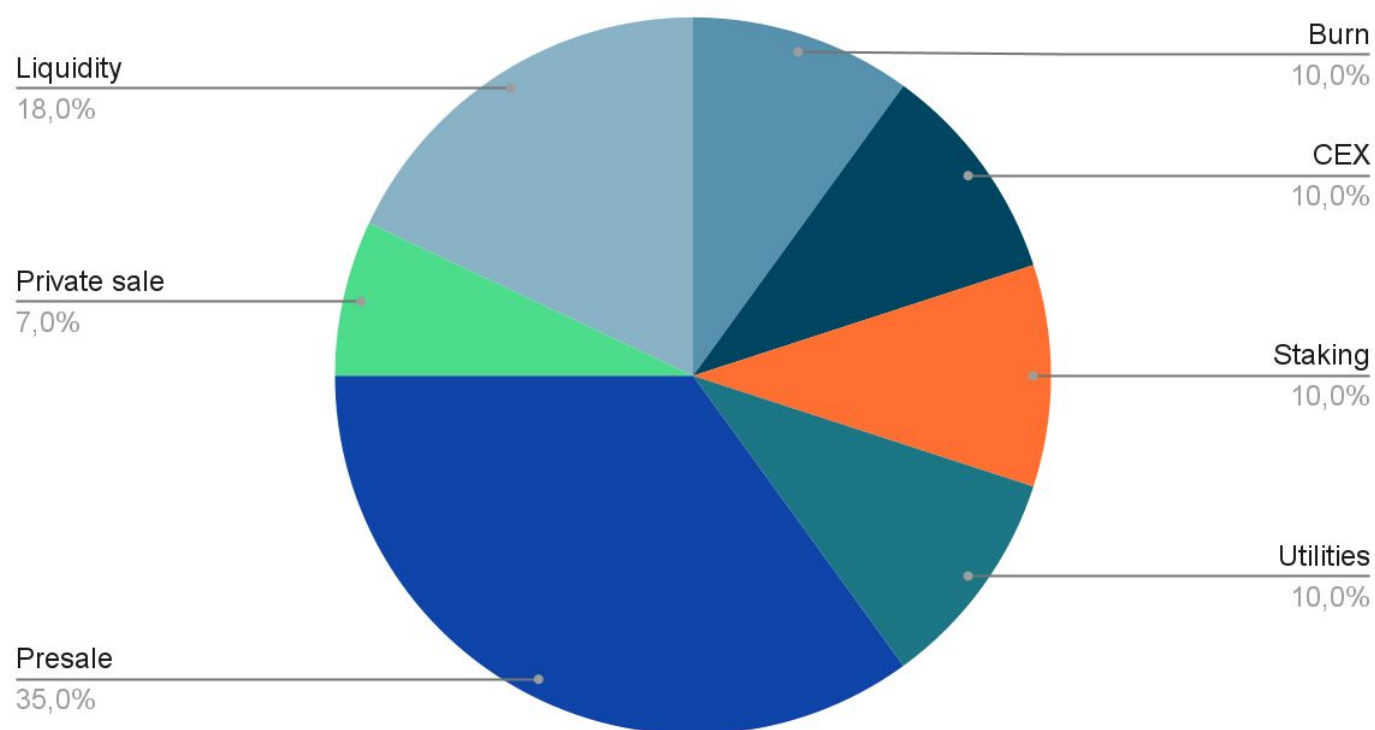
Summer Doge
GOOD PRACTICES FOUND

✔ The owner cannot mint new tokens after deployment

07

The following tokenomics are based on the project's whitepaper and/or website:

- 35% - Presale
- 7% - Private sale
- 18% - Liquidity
- 10% - Utilities
- 10% - Burn
- 10% - CEX
- 10% - Staking

Tokens distribution

Burn
10,0%

CEX
10,0%

Staking
10,0%

Utilities
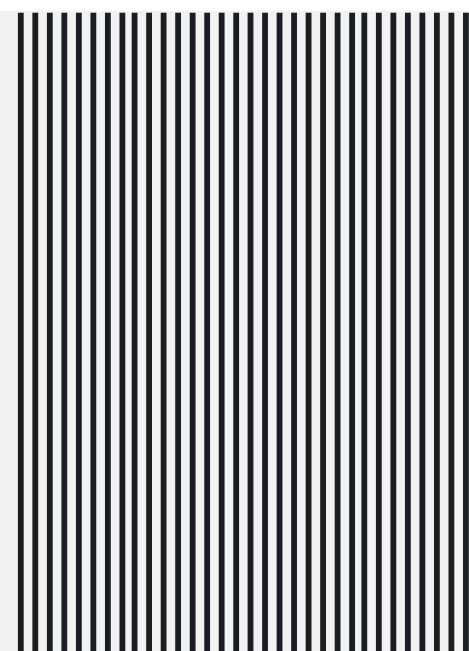10,0%

Presale
35,0%

Private sale
7,0%

Liquidity
18,0%

THE TEAM

The team has privately doxxed to PINKSALE

https://pinksale.notion.site/Summer-Doge-KYC-Verification-7cef58e459984888a502824694a3a50d?pvs=4

Summer Doge - KYC Verification

This KYC page verifies that **One Member** of the project has successfully completed the verification process at PinkSale. Project info:

- Project Name: Summer Doge
- Project Website: https://summerdoge.xyz/
- KYC Issued: July 12, 2023

Disclaimer

A project receiving the KYC badge does not mean in any way that we approve or recommend that project, even if we host an AMA with them. Please always DYOR before investing, remembering that PinkSale is a decentralized platform.

09

Website URL
https://summerdoge.xyz/

Domain Registry
https://www.ovh.com

Domain Expiration
2024-07-04

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Yes, explanatory.

Roadmap
Yes, goals set without time frames.
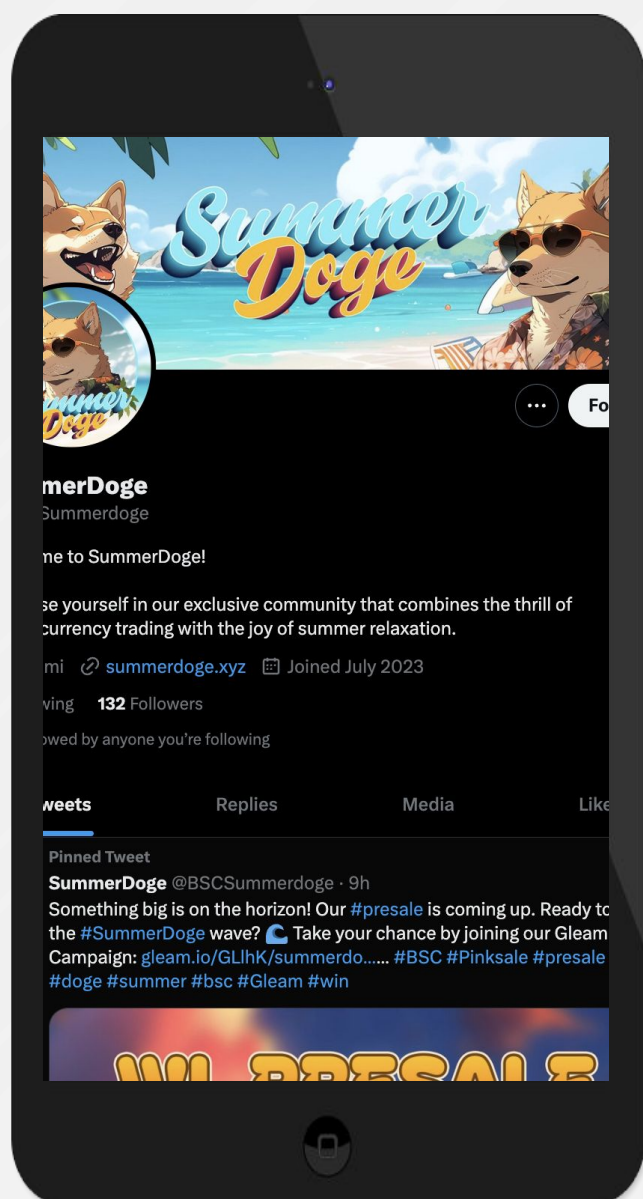
Mobile-friendly?
Yes

summerdoge.xyz

SOCIAL MEDIA
& ONLINE PRESENCE
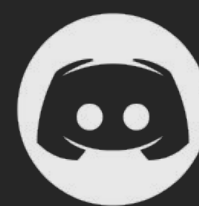
Twitter

@BSCSummerdoge

- 109 followers
- Active
- Posts frequently

Discord

- Not available

Telegram

@SummerDogePortalOfficial

- 739 members
- Active members
- Active mods

Medium

- Not available

11

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 500 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 500 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 SPYWOLF.CO

✈ @SPYWOLFNETWORK

🐦 @SPYWOLFNETWORK

12

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.